



# ISC2

## Exam Questions CISSP

Certified Information Systems Security Professional (CISSP)

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

- (Exam Topic 15)

What is the MAIN objective of risk analysis in Disaster Recovery (DR) planning?

- A. Establish Maximum Tolerable Downtime (MTD) Information Systems (IS).
- B. Define the variable cost for extended downtime scenarios.
- C. Identify potential threats to business availability.
- D. Establish personnel requirements for various downtime scenarios.

**Answer: C**

#### NEW QUESTION 2

- (Exam Topic 15)

An organization is planning a penetration test that simulates the malicious actions of a former network administrator. What kind of penetration test is needed?

- A. Functional test
- B. Unit test
- C. Grey box
- D. White box

**Answer: C**

#### NEW QUESTION 3

- (Exam Topic 15)

In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

- A. Organizational Security Policy
- B. Security Target (ST)
- C. Protection Profile (PP)
- D. Target of Evaluation (TOE)

**Answer: C**

#### NEW QUESTION 4

- (Exam Topic 15)

Which of the following is the top barrier for companies to adopt cloud technology?

- A. Migration period
- B. Data integrity
- C. Cost
- D. Security

**Answer: D**

#### NEW QUESTION 5

- (Exam Topic 15)

Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

- A. Proper security controls, security goals, and fault mitigation are properly conducted.
- B. Proper security controls, security objectives, and security goals are properly initiated.
- C. Security goals, proper security controls, and validation are properly initiated.
- D. Security objectives, security goals, and system test are properly conducted.

**Answer: B**

#### NEW QUESTION 6

- (Exam Topic 15)

The security architect is designing and implementing an internal certification authority to generate digital certificates for all employees. Which of the following is the BEST solution to securely store the private keys?

- A. Physically secured storage device
- B. Encrypted flash drive
- C. Public key infrastructure (PKI)
- D. Trusted Platform Module (TPM)

**Answer: C**

#### NEW QUESTION 7

- (Exam Topic 15)

Two computers, each with a single connection on the same physical 10 gigabit Ethernet network segment, need to communicate with each other. The first machine has a single Internet Protocol (IP) Classless Inter-Domain Routing (CIDR) address of 192.168.1.3/30 and the second machine has an IP/CIDR address 192.168.1.6/30. Which of the following is correct?

- A. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network bridge in order to communicate.
- B. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network bridge in order to communicate.

- C. Since each computer is on the same layer 3 network, traffic between the computers may be processed by a network router in order to communicate.
- D. Since each computer is on a different layer 3 network, traffic between the computers must be processed by a network router in order to communicate.

**Answer:** B

#### NEW QUESTION 8

- (Exam Topic 15)

While reviewing the financial reporting risks of a third-party application, which of the following Service Organization Control (SOC) reports will be the MOST useful?

- A. ISIsOC 1
- B. SOC 2
- C. SOC 3
- D. SOC for cybersecurity

**Answer:** A

#### NEW QUESTION 9

- (Exam Topic 15)

Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-systems gracefully handle invalid input?

- A. Unit testing
- B. Integration testing
- C. Negative testing
- D. Acceptance testing

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 15)

he security organization is loading for a solution that could help them determine with a strong level of confident that attackers have breached their network. Which solution is MOST effective at discovering successful network breach?

- A. Installing an intrusion prevention system (IPS)
- B. Deploying a honeypot
- C. Installing an intrusion detection system (IDS)
- D. Developing a sandbox

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 15)

Which of the following access control models is MOST restrictive?

- A. Discretionary Access Control (DAC)
- B. Mandatory Access Control (MAC)
- C. Role Based Access Control (RBAC)
- D. Rule based access control

**Answer:** B

#### NEW QUESTION 15

- (Exam Topic 15)

A breach investigation ..... a website was exploited through an open sourced .....Is The FIRB Stan In the Process that could have prevented this breach?

- A. Application whitelisting
- B. Web application firewall (WAF)
- C. Vulnerability remediation
- D. Software inventory

**Answer:** B

#### NEW QUESTION 18

- (Exam Topic 15)

Which of the following is the FIRST step for defining Service Level Requirements (SLR)?

- A. Creating a prototype to confirm or refine the customer requirements
- B. Drafting requirements for the service level agreement (SLA)
- C. Discussing technology and solution requirements with the customer
- D. Capturing and documenting the requirements of the customer

**Answer:** D

#### NEW QUESTION 20

- (Exam Topic 15)

Which of the following provides the MOST secure method for Network Access Control (NAC)?

- A. Media Access Control (MAC) filtering
- B. 802.IX authentication
- C. Application layer filtering
- D. Network Address Translation (NAT)

**Answer:** B

#### NEW QUESTION 22

- (Exam Topic 15)

During a penetration test, what are the three PRIMARY objectives of the planning phase?

- A. Determine testing goals, identify rules of engagement, and conduct an initial discovery scan.
- B. Finalize management approval, determine testing goals, and gather port and service information.
- C. Identify rules of engagement, finalize management approval, and determine testing goals.
- D. Identify rules of engagement, document management approval, and collect system and application information.

**Answer:** D

#### NEW QUESTION 27

- (Exam Topic 15)

An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP). The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract.

Which of the following MUST be included in the contract?

- A. A detailed overview of all equipment involved in the outsourcing contract
- B. The MSSP having an executive manager responsible for information security
- C. The right to perform security compliance tests on the MSSP's equipment
- D. The right to audit the MSSP's security process

**Answer:** C

#### NEW QUESTION 32

- (Exam Topic 15)

Which of the following ensures old log data is not overwritten?

- A. Increase log file size
- B. Implement Syslog
- C. Log preservation
- D. Log retention

**Answer:** D

#### NEW QUESTION 37

- (Exam Topic 15)

In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed?

- A. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
- B. Maintain and improve the Business Continuity Management (BCM) system by taking corrective action, based on the results of management review.
- C. Ensure the business continuity policy, controls, processes, and procedures have been implemented.
- D. Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established.

**Answer:** D

#### NEW QUESTION 40

- (Exam Topic 15)

Which of the following is a common term for log reviews, synthetic transactions, and code reviews?

- A. Security control testing
- B. Application development
- C. Spiral development functional testing
- D. DevOps Integrated Product Team (IPT) development

**Answer:** B

#### NEW QUESTION 42

- (Exam Topic 15)

Which of the following is the BEST way to protect an organization's data assets?

- A. Monitor and enforce adherence to security policies.
- B. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.
- C. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.
- D. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

**Answer:** B

#### NEW QUESTION 44

- (Exam Topic 15)

What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

- A. ICS often do not have availability requirements.
- B. ICS are often isolated and difficult to access.
- C. ICS often run on UNIX operating systems.
- D. ICS are often sensitive to unexpected traffic.

**Answer:** B

#### NEW QUESTION 49

- (Exam Topic 15)

A customer continues to experience attacks on their email, web, and File Transfer Protocol (FTP) servers. These attacks are impacting their business operations. Which of the following is the BEST recommendation to make?

- A. Configure an intrusion detection system (IDS).
- B. Create a demilitarized zone (DMZ).
- C. Deploy a bastion host.
- D. Setup a network firewall.

**Answer:** C

#### NEW QUESTION 53

- (Exam Topic 15)

What type of database attack would allow a customer service employee to determine quarterly sales results before they are publically announced?

- A. Polyinstantiation
- B. Inference
- C. Aggregation
- D. Data mining

**Answer:** A

#### NEW QUESTION 54

- (Exam Topic 15)

What is the MAIN purpose of conducting a business impact analysis (BIA)?

- A. To determine the critical resources required to recover from an incident within a specified time period
- B. To determine the effect of mission-critical information system failures on core business processes
- C. To determine the cost for restoration of damaged information system
- D. To determine the controls required to return to business critical operations

**Answer:** B

#### NEW QUESTION 55

- (Exam Topic 15)

An organization needs a general purpose document to prove that its internal controls properly address security, availability, processing integrity, confidentiality or privacy risks. Which of the following reports is required?

- A. A Service Organization Control (SOC) 3 report
- B. The Statement on Standards for Attestation Engagements N
- C. 18 (SSAE 18)
- D. A Service Organization Control (SOC) 2 report
- E. The International Organization for Standardization (ISO) 27001

**Answer:** C

#### NEW QUESTION 60

- (Exam Topic 15)

During a Disaster Recovery (DR) simulation, it is discovered that the shared recovery site lacks adequate data restoration capabilities to support the implementation of multiple plans simultaneously. What would be impacted by this fact if left unchanged?

- A. Recovery Point Objective (RPO)
- B. Recovery Time Objective (RTO)
- C. Business Impact Analysis (BIA)
- D. Return on Investment (ROI)
- E. A

**Answer:** E

#### NEW QUESTION 63

- (Exam Topic 15)

What is the FIRST step for an organization to take before allowing personnel to access social media from a corporate device or user account?

- A. Publish a social media guidelines document.

- B. Publish an acceptable usage policy.
- C. Document a procedure for accessing social media sites.
- D. Deliver security awareness training.

**Answer:** A

#### NEW QUESTION 65

- (Exam Topic 15)

Recently, an unknown event has disrupted a single Layer-2 network that spans between two geographically diverse data centers. The network engineers have asked for assistance in identifying the root cause of the event. Which of the following is the MOST likely cause?

- A. Misconfigured routing protocol
- B. Smurf attack
- C. Broadcast domain too large
- D. Address spoofing

**Answer:** D

#### NEW QUESTION 66

- (Exam Topic 15)

What would be the BEST action to take in a situation where collected evidence was left unattended overnight in an unlocked vehicle?

- A. Report the matter to the local police authorities.
- B. Move evidence to a climate-controlled environment.
- C. Re-inventory the evidence and provide it to the evidence custodian.
- D. Immediately report the matter to the case supervisor.

**Answer:** D

#### NEW QUESTION 69

- (Exam Topic 15)

Which of the following is the MOST effective method of detecting vulnerabilities in web-based applications early in the secure Software Development Life Cycle (SDLC)?

- A. Web application vulnerability scanning
- B. Application fuzzing
- C. Code review
- D. Penetration testing

**Answer:** C

#### NEW QUESTION 70

- (Exam Topic 15)

Which of the following security objectives for industrial control systems (ICS) can be adapted to securing any Internet of Things (IoT) system?

- A. Prevent unauthorized modification of data.
- B. Restore the system after an incident.
- C. Detect security events and incidents.
- D. Protect individual components from exploitation

**Answer:** D

#### NEW QUESTION 75

- (Exam Topic 15)

In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

- A. Prepare to take corrective actions quickly.
- B. Receive approval from the change review board.
- C. Review logs for any anomalies.
- D. Automate functionality testing.

**Answer:** B

#### NEW QUESTION 79

- (Exam Topic 15)

Why is authentication by ownership stronger than authentication by knowledge?

- A. It is easier to change.
- B. It can be kept on the user's person.
- C. It is more difficult to duplicate.
- D. It is simpler to control.

**Answer:** B

#### NEW QUESTION 84



- (Exam Topic 15)

Which of the following types of firewall only examines the “handshaking” between packets before forwarding traffic?

- A. Proxy firewalls
- B. Host-based firewalls
- C. Circuit-level firewalls
- D. Network Address Translation (NAT) firewalls

**Answer:** C

#### NEW QUESTION 88

- (Exam Topic 15)

A digitally-signed e-mail was delivered over a wireless network protected with Wired Equivalent Privacy (WEP) protocol. Which of the following principles is at risk?

- A. Availability
- B. Non-Repudiation
- C. Confidentiality
- D. Integrity

**Answer:** B

#### NEW QUESTION 90

- (Exam Topic 15)

What method could be used to prevent passive attacks against secure voice communications between an organization and its vendor?

- A. Encryption in transit
- B. Configure a virtual private network (VPN)
- C. Configure a dedicated connection
- D. Encryption at rest

**Answer:** A

#### NEW QUESTION 91

- (Exam Topic 15)

Which of the following is an indicator that a company's new user security awareness training module has been effective?

- A. There are more secure connections to the internal database servers.
- B. More incidents of phishing attempts are being reported.
- C. There are more secure connections to internal e-mail servers.
- D. Fewer incidents of phishing attempts are being reported.

**Answer:** B

#### NEW QUESTION 93

- (Exam Topic 15)

Which element of software supply chain management has the GREATEST security risk to organizations?

- A. New software development skills are hard to acquire.
- B. Unsupported libraries are often used.
- C. Applications with multiple contributors are difficult to evaluate.
- D. Vulnerabilities are difficult to detect.

**Answer:** B

#### NEW QUESTION 95

- (Exam Topic 15)

Who should formulate conclusions from a particular digital fore Ball, Submit a Toper Of Tags, and the results?

- A. The information security professional's supervisor
- B. Legal counsel for the information security professional's employer
- C. The information security professional who conducted the analysis
- D. A peer reviewer of the information security professional

**Answer:** B

#### NEW QUESTION 100

- (Exam Topic 15)

Which of the following actions should be taken by a security professional when a mission critical computer network attack is suspected?

- A. Isolate the network, log an independent report, fix the problem, and redeploy the computer.
- B. Isolate the network, install patches, and report the occurrence.
- C. Prioritize, report, and investigate the occurrence.
- D. Turn the router off, perform forensic analysis, apply the appropriate fin, and log incidents.

**Answer:** C



#### NEW QUESTION 103

- (Exam Topic 15)

A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

- A. Availability
- B. Disaster recovery (DR)
- C. Redundancy
- D. Business continuity (BC)

**Answer:** D

#### NEW QUESTION 106

- (Exam Topic 15)

An establish information technology (IT) consulting firm is considering acquiring a successful local startup. To gain a comprehensive understanding of the startup's security posture' which type of assessment provides the BEST information?

- A. A security audit
- B. A penetration test
- C. A tabletop exercise
- D. A security threat model

**Answer:** A

#### NEW QUESTION 107

- (Exam Topic 15)

Which of the following is the GREATEST risk of relying only on Capability Maturity Models (CMM) for software to guide process improvement and assess capabilities of acquired software?

- A. Organizations can only reach a maturity level 3 when using CMMs
- B. CMMs do not explicitly address safety and security
- C. CMMs can only be used for software developed in-house
- D. CMMs are vendor specific and may be biased

**Answer:** B

#### NEW QUESTION 112

- (Exam Topic 15)

A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

- A. Virtual network computing
- B. Secure Socket Shell
- C. in-band connection
- D. Site-to-site VPN

**Answer:** D

#### NEW QUESTION 113

- (Exam Topic 15)

Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

- A. Data at rest has been compromised when the user has authenticated to the device.
- B. Data on the device cannot be restored from backup.
- C. Data in transit has been compromised when the user has authenticated to the device.
- D. Data on the device cannot be backed up.

**Answer:** A

#### NEW QUESTION 116

- (Exam Topic 15)

Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

- A. Directory
- B. User database
- C. Multi-factor authentication (MFA)
- D. Single sign-on (SSO)

**Answer:** A

#### NEW QUESTION 120

- (Exam Topic 15)

Spyware is BEST described as

- A. data mining for advertising.
- B. a form of cyber-terrorism,

- C. an information gathering technique,
- D. a web-based attack.

**Answer:** B

#### NEW QUESTION 124

- (Exam Topic 15)

Which of the following is the MOST important rule for digital investigations?

- A. Ensure event logs are rotated.
- B. Ensure original data is never modified.
- C. Ensure individual privacy is protected.
- D. Ensure systems are powered on.

**Answer:** C

#### NEW QUESTION 125

- (Exam Topic 15)

When configuring Extensible Authentication Protocol (EAP) in a Voice over Internet Protocol (VoIP) network, which of the following authentication types is the MOST secure?

- A. EAP-Transport Layer Security (TLS)
- B. EAP-Flexible Authentication via Secure Tunneling
- C. EAP-Tunneled Transport Layer Security (TLS)
- D. EAP-Protected Extensible Authentication Protocol (PEAP)

**Answer:** C

#### NEW QUESTION 128

- (Exam Topic 15)

What is the term used to define where data is geographically stored in the cloud?

- A. Data warehouse
- B. Data privacy rights
- C. Data subject rights
- D. Data sovereignty

**Answer:** D

#### NEW QUESTION 129

- (Exam Topic 15)

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

- A. Omni
- B. Directional
- C. Yagi
- D. Parabolic

**Answer:** A

#### NEW QUESTION 131

- (Exam Topic 15)

A developer begins employment with an information technology (IT) organization. On the first day, the developer works through the list of assigned projects and finds that some files within those projects aren't accessible. Other developers working on the same project have no trouble locating and working on the. What is the MOST likely explanation for the discrepancy in access?

- A. The IT administrator had failed to grant the developer privileged access to the servers.
- B. The project files were inadvertently deleted.
- C. The new developer's computer had not been added to an access control list (ACL).
- D. The new developer's user account was not associated with the right roles needed for the projects.

**Answer:** A

#### NEW QUESTION 134

- (Exam Topic 15)

A client server infrastructure that provides user-to-server authentication describes which one of the following?

- A. Secure Sockets Layer (SSL)
- B. Kerberos
- C. 509
- D. User-based authorization

**Answer:** B

#### NEW QUESTION 139

- (Exam Topic 15)

In which of the following system life cycle processes should security requirements be developed?

- A. Risk management
- B. Business analysis
- C. Information management
- D. System analysis

**Answer: B**

#### NEW QUESTION 144

- (Exam Topic 15)

Information Security Continuous Monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

- A. Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- B. Conduct a vulnerability assessment to discover current threats against the environment and incorporate them into the program.
- C. Respond to findings with technical management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- D. Analyze the data collected and report findings, determining the appropriate responses
- E. It may be necessary to collect additional information to clarify or supplement existing monitoring data.

**Answer: A**

#### NEW QUESTION 149

- (Exam Topic 15)

Which of the following criteria ensures information is protected relative to its importance to the organization?

- A. The value of the data to the organization's senior management
- B. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification
- C. Legal requirements determined by the organization headquarters' location
- D. Organizational stakeholders, with classification approved by the management board

**Answer: D**

#### NEW QUESTION 151

- (Exam Topic 15)

Which of the following are the BEST characteristics of security metrics?

- A. They are generalized and provide a broad overview
- B. They use acronyms and abbreviations to be concise
- C. They use bar charts and Venn diagrams
- D. They are consistently measured and quantitatively expressed

**Answer: D**

#### NEW QUESTION 152

- (Exam Topic 15)

Which of the following is a Key Performance Indicator (KPI) for a security training and awareness program?

- A. The number of security audits performed
- B. The number of attendees at security training events
- C. The number of security training materials created
- D. The number of security controls implemented

**Answer: B**

#### NEW QUESTION 156

- (Exam Topic 15)

- A. Obtain information security management approval.
- B. Maintain the integrity of the application.
- C. Obtain feedback before implementation.
- D. Identify vulnerabilities.

**Answer: D**

#### NEW QUESTION 161

- (Exam Topic 15)

Which of the following is the MOST appropriate control for asset data labeling procedures?

- A. Logging data media to provide a physical inventory control
- B. Reviewing audit trails of logging records
- C. Categorizing the types of media being used
- D. Reviewing off-site storage access controls

**Answer:** C

**NEW QUESTION 162**

- (Exam Topic 15)

The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

- A. Security information and event management (SIEM)
- B. Security perimeter
- C. Defense-in-depth
- D. Access control

**Answer:** B

**NEW QUESTION 167**

- (Exam Topic 15)

An information technology (IT) employee who travels frequently to various sites remotely to an organization's the following solutions BEST serves as a secure control mechanism to meet the organization's requirements? to troubleshoot p Which of the following solutions BEST serves as a secure control mechanism to meet the organization's requirements?

- A. Update the firewall rules to include the static Internet Protocol (IP) addresses of the locations where the employee connects from.
- B. Install a third-party screen sharing solution that provides remote connection from a public website.
- C. Implement a Dynamic Domain Name Services (DDNS) account to initiate a virtual private network (VPN) using the DDNS record.
- D. Install a bastion host in the demilitarized zone (DMZ) and allow multi-factor authentication (MFA) access.

**Answer:** D

**NEW QUESTION 171**

- (Exam Topic 15)

Which of the following is the BEST way to determine the success of a patch management process?

- A. Analysis and impact assessment
- B. Auditing and assessment
- C. Configuration management (CM)
- D. Change management

**Answer:** A

**NEW QUESTION 173**

- (Exam Topic 15)

Which type of disaster recovery plan (DRP) testing carries the MOST operational risk?

- A. Cutover
- B. Walkthrough
- C. Tabletop
- D. Parallel

**Answer:** C

**NEW QUESTION 174**

- (Exam Topic 15)

If the wide area network (WAN) is supporting converged applications like Voice over Internet Protocol (VoIP), which of the following becomes even MORE essential to the assurance of network?

- A. Classless Inter-Domain Routing (CIDR)
- B. Deterministic routing
- C. Internet Protocol (IP) routing lookups
- D. Boundary routing

**Answer:** C

**NEW QUESTION 179**

- (Exam Topic 15)

Which of the following terms BEST describes a system which allows a user to log in and access multiple related servers and applications?

- A. Remote Desktop Protocol (RDP)
- B. Federated identity management (FIM)
- C. Single sign-on (SSO)
- D. Multi-factor authentication (MFA)

**Answer:** B

**NEW QUESTION 181**

- (Exam Topic 15)

What is the MINIMUM standard for testing a disaster recovery plan (DRP)?

- A. Semi-annually and in alignment with a fiscal half-year business cycle
- B. Annually or less frequently depending upon audit department requirements
- C. Quarterly or more frequently depending upon the advice of the information security manager
- D. As often as necessary depending upon the stability of the environment and business requirements

**Answer:** D

#### NEW QUESTION 182

- (Exam Topic 15)

Which of the following poses the GREATEST privacy risk to personally identifiable information (PII) when disposing of an office printer or copier?

- A. The device could contain a document with PII on the platen glass
- B. Organizational network configuration information could still be present within the device
- C. A hard disk drive (HDD) in the device could contain PII
- D. The device transfer roller could contain imprints of PII

**Answer:** B

#### NEW QUESTION 186

- (Exam Topic 15)

In systems security engineering, what does the security principle of modularity provide?

- A. Documentation of functions
- B. Isolated functions and data
- C. Secure distribution of programs and data
- D. Minimal access to perform a function

**Answer:** A

#### NEW QUESTION 187

- (Exam Topic 15)

An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

- A. IM clients can interoperate between multiple vendors.
- B. IM clients can run without administrator privileges.
- C. IM clients can utilize random port numbers.
- D. IM clients can run as executable that do not require installation.

**Answer:** B

#### NEW QUESTION 189

- (Exam Topic 15)

The personal laptop of an organization executive is stolen from the office, complete with personnel and project records. Which of the following should be done FIRST to mitigate future occurrences?

- A. Encrypt disks on personal laptops.
- B. Issue cable locks for use on personal laptops.
- C. Create policies addressing critical information on personal laptops.
- D. Monitor personal laptops for critical information.

**Answer:** A

#### NEW QUESTION 190

- (Exam Topic 15)

An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

- A. It should be expressed as general requirements.
- B. It should be expressed in legal terminology.
- C. It should be expressed in business terminology.
- D. It should be expressed as technical requirements.

**Answer:** D

#### NEW QUESTION 191

- (Exam Topic 15)

What BEST describes the confidentiality, integrity, availability triad?

- A. A tool used to assist in understanding how to protect the organization's data
- B. The three-step approach to determine the risk level of an organization
- C. The implementation of security systems to protect the organization's data
- D. A vulnerability assessment to see how well the organization's data is protected

**Answer:** C

#### NEW QUESTION 194

- (Exam Topic 15)

A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

- A. Arraignment
- B. Trial
- C. Sentencing
- D. Discovery

**Answer:** D

#### NEW QUESTION 196

- (Exam Topic 15)

Which of the following security tools monitors devices and records the information in a central database for further analysis?

- A. Security orchestration automation and response
- B. Host-based intrusion detection system (HIDS)
- C. Antivirus
- D. Endpoint detection and response (EDR)

**Answer:** A

#### NEW QUESTION 201

- (Exam Topic 15)

What is the FINAL step in the waterfall method for contingency planning?

- A. Maintenance
- B. Testing
- C. Implementation
- D. Training

**Answer:** A

#### NEW QUESTION 203

- (Exam Topic 15)

What is static analysis intended to do when analyzing an executable file?

- A. Collect evidence of the executable file's usage, including dates of creation and last use.
- B. Search the documents and files associated with the executable file.
- C. Analyze the position of the file in the file system and the executable file's libraries.
- D. Disassemble the file to gather information about the executable file's function.

**Answer:** D

#### NEW QUESTION 204

- (Exam Topic 15)

What is the benefit of using Network Admission Control (NAC)?

- A. Operating system (OS) versions can be validated prior to allowing network access.
- B. NAC supports validation of the endpoint's security posture prior to allowing the session to go into an authorized state.
- C. NAC can require the use of certificates, passwords, or a combination of both before allowing network admission.
- D. NAC only supports Windows operating systems (OS).

**Answer:** C

#### NEW QUESTION 208

- (Exam Topic 15)

Which of the following minimizes damage to information technology (IT) equipment stored in a data center when a false fire alarm event occurs?

- A. A pre-action system is installed.
- B. An open system is installed.
- C. A dry system is installed.
- D. A wet system is installed.

**Answer:** C

#### NEW QUESTION 209

- (Exam Topic 15)

Which of the following is the PRIMARY issue when analyzing detailed log information?

- A. Logs may be unavailable when required
- B. Timely review of the data is potentially difficult
- C. Most systems and applications do not support logging
- D. Logs do not provide sufficient details of system and individual activities

**Answer:** D



#### NEW QUESTION 210

- (Exam Topic 15)

Which of the following describes the order in which a digital forensic process is usually conducted?

- A. Ascertain legal authority, agree upon examination strategy, conduct examination, and report results
- B. Ascertain legal authority, conduct investigation, report results, and agree upon examination strategy
- C. Agree upon examination strategy, ascertain legal authority, conduct examination, and report results
- D. Agree upon examination strategy, ascertain legal authority, report results, and conduct examination

**Answer:** A

#### NEW QUESTION 214

- (Exam Topic 15)

Which of the following addresses requirements of security assessments during software acquisition?

- A. Software configuration management (SCM)
- B. Data loss prevention (DLP) policy
- C. Continuous monitoring
- D. Software assurance policy

**Answer:** A

#### NEW QUESTION 217

- (Exam Topic 15)

Which of the following will an organization's network vulnerability testing process BEST enhance?

- A. Firewall log review processes
- B. Asset management procedures
- C. Server hardening processes
- D. Code review procedures

**Answer:** C

#### NEW QUESTION 221

- (Exam Topic 15)

Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this TAM action?

- A. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to services.
- B. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to services.
- C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identityprovider (IdP) and allows access to resources.
- D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a ServiceProvider and allows access to resources.

**Answer:** A

#### NEW QUESTION 224

- (Exam Topic 15)

Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

- A. File Integrity Checker
- B. Security information and event management (SIEM) system
- C. Audit Logs
- D. Intrusion detection system (IDS)

**Answer:** A

#### NEW QUESTION 228

- (Exam Topic 15)

What are the essential elements of a Risk Assessment Report (RAR)?

- A. Table of contents, testing criteria, and index
- B. Table of contents, chapters, and executive summary
- C. Executive summary, graph of risks, and process
- D. Executive summary, body of the report, and appendices

**Answer:** D

#### NEW QUESTION 231

- (Exam Topic 15)

When defining a set of security controls to mitigate a risk, which of the following actions MUST occur?



- A. Each control's effectiveness must be evaluated individually.
- B. Each control must completely mitigate the risk.
- C. The control set must adequately mitigate the risk.
- D. The control set must evenly divided the risk.

**Answer:** A

#### NEW QUESTION 235

- (Exam Topic 15)

An organization is planning to have an it audit of its as a Service (SaaS) application to demonstrate to external parties that the security controls around availability are designed. The audit report must also cover a certain period of time to show the operational effectiveness of the controls. Which Service Organization Control (SOC) report would BEST fit their needs?

- A. SOC 1 Type 1
- B. SOC 1 Type 2
- C. SOC 2 Type 1
- D. SOC 2 Type 2

**Answer:** D

#### NEW QUESTION 236

- (Exam Topic 15)

A Distributed Denial of Service (DDoS) attack was carried out using malware called Mirai to create a large-scale command and control system to launch a botnet. Which of the following devices were the PRIMARY sources used to generate the attack traffic?

- A. Internet of Things (IoT) devices
- B. Microsoft Windows hosts
- C. Web servers running open source operating systems (OS)
- D. Mobile devices running Android

**Answer:** A

#### NEW QUESTION 241

- (Exam Topic 15)

Which of the following is the BEST approach to implement multiple servers on a virtual system?

- A. Implement multiple functions per virtual server and apply the same security configuration for each virtual server.
- B. Implement one primary function per virtual server and apply high security configuration on the host operating system.
- C. Implement one primary function per virtual server and apply individual security configuration for each virtual server.
- D. Implement multiple functions within the same virtual server and apply individual security configurations to each function.

**Answer:** C

#### NEW QUESTION 245

- (Exam Topic 15)

Which of the following is required to verify the authenticity of a digitally signed document?

- A. Digital hash of the signed document
- B. Sender's private key
- C. Recipient's public key
- D. Agreed upon shared secret

**Answer:** A

#### NEW QUESTION 246

- (Exam Topic 15)

An organization has determined that its previous waterfall approach to software development is not keeping pace with business demands. To adapt to the rapid changes required for product delivery, the organization has decided to move towards an Agile software development and release cycle. In order to ensure the success of the Agile methodology, who is MOST critical in creating acceptance tests or acceptance criteria for each release?

- A. Project managers
- B. Software developers
- C. Independent testers
- D. Business customers

**Answer:** D

#### NEW QUESTION 251

- (Exam Topic 15)

Which of the following is the PRIMARY goal of logical access controls?

- A. Restrict access to an information asset.
- B. Ensure integrity of an information asset.
- C. Restrict physical access to an information asset.
- D. Ensure availability of an information asset.

**Answer:** C

#### NEW QUESTION 253

- (Exam Topic 15)

Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

- A. Sniffing the traffic of a compromised host inside the network
- B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network
- C. A brute force password attack on the Secure Shell (SSH) port of the controller
- D. Remote Authentication Dial-In User Service (RADIUS) token replay attack

**Answer: B**

#### NEW QUESTION 255

- (Exam Topic 15)

Which of the following would be the BEST mitigation practice for man-in-the-middle (MITM) Voice over Internet Protocol (VoIP) attacks?

- A. Use Media Gateway Control Protocol (MGCP)
- B. Use Transport Layer Security (TLS) protocol
- C. Use File Transfer Protocol (FTP)
- D. Use Secure Shell (SSH) protocol

**Answer: B**

#### NEW QUESTION 260

- (Exam Topic 15)

A company hired an external vendor to perform a penetration test of a new payroll system. The company's internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

- A. Failure to perform interface testing
- B. Failure to perform negative testing
- C. Inadequate performance testing
- D. Inadequate application level testing

**Answer: A**

#### NEW QUESTION 265

- (Exam Topic 15)

The ability to send malicious code, generally in the form of a client side script, to a different end user is categorized as which type of vulnerability?

- A. Session hijacking
- B. Cross-site request forgery (CSRF)
- C. Cross-Site Scripting (XSS)
- D. Command injection

**Answer: C**

#### NEW QUESTION 267

- (Exam Topic 15)

Where can the Open Web Application Security Project (OWASP) list of associated vulnerabilities be found?

- A. OWASP Top 10 Project
- B. OWASP Software Assurance Maturity Model (SAMM) Project
- C. OWASP Guide Project
- D. OWASP Mobile Project

**Answer: A**

#### NEW QUESTION 268

- (Exam Topic 15)

Which of the following is considered the FIRST step when designing an internal security control assessment?

- A. Create a plan based on recent vulnerability scans of the systems in question.
- B. Create a plan based on comprehensive knowledge of known breaches.
- C. Create a plan based on a recognized framework of known controls.
- D. Create a plan based on reconnaissance of the organization's infrastructure.

**Answer: D**

#### NEW QUESTION 269

- (Exam Topic 15)

Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

- A. Multiprotocol Label Switching (MPLS)
- B. Synchronous Optical Networking (SONET)
- C. Session Initiation Protocol (SIP)

D. Fiber Channel Over Ethernet (FCoE)

**Answer:** A

#### NEW QUESTION 271

- (Exam Topic 15)

A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

- A. Pinning
- B. Single-pass wipe
- C. Degaussing
- D. Multi-pass wipes

**Answer:** C

#### NEW QUESTION 276

- (Exam Topic 15)

What is a risk of using commercial off-the-shelf (COTS) products?

- A. COTS products may not map directly to an organization's security requirements.
- B. COTS products are typically more expensive than developing software in-house.
- C. Cost to implement COTS products is difficult to predict.
- D. Vendors are often hesitant to share their source code.

**Answer:** A

#### NEW QUESTION 280

- (Exam Topic 15)

The Open Web Application Security Project's (OWASP) Software Assurance Maturity Model (SAMM) allows organizations to implement a flexible software security strategy to measure organizational impact based on what risk management aspect?

- A. Risk tolerance
- B. Risk exception
- C. Risk treatment
- D. Risk response

**Answer:** D

#### NEW QUESTION 282

- (Exam Topic 15)

Which of the following BEST describes the purpose of software forensics?

- A. To perform cyclic redundancy check (CRC) verification and detect changed applications
- B. To review program code to determine the existence of backdoors
- C. To analyze possible malicious intent of malware
- D. To determine the author and behavior of the code

**Answer:** D

#### NEW QUESTION 285

- (Exam Topic 15)

A software architect has been asked to build a platform to distribute music to thousands of users on a global scale. The architect has been reading about content delivery networks (CDN). Which of the following is a principal task to undertake?

- A. Establish a service-oriented architecture (SOA).
- B. Establish a media caching methodology.
- C. Establish relationships with hundreds of Internet service providers (ISP).
- D. Establish a low-latency wide area network (WAN).

**Answer:** B

#### NEW QUESTION 290

- (Exam Topic 15)

An organization's retail website provides its only source of revenue, so the disaster recovery plan (DRP) must document an estimated time for each step in the plan.

Which of the following steps in the DRP will list the GREATEST duration of time for the service to be fully operational?

- A. Update the Network Address Translation (NAT) table.
- B. Update Domain Name System (DNS) server addresses with domain registrar.
- C. Update the Border Gateway Protocol (BGP) autonomous system number.
- D. Update the web server network adapter configuration.

**Answer:** B

#### NEW QUESTION 294

- (Exam Topic 15)

What is the MOST significant benefit of role-based access control (RBAC)?

- A. Reduction in authorization administration overhead
- B. Reduces inappropriate access
- C. Management of least privilege
- D. Most granular form of access control

**Answer:** A

#### NEW QUESTION 298

- (Exam Topic 15)

Which of the following BEST obtains an objective audit of security controls?

- A. The security audit is measured against a known standard.
- B. The security audit is performed by a certified internal auditor.
- C. The security audit is performed by an independent third-party.
- D. The security audit produces reporting metrics for senior leadership.

**Answer:** A

#### NEW QUESTION 302

- (Exam Topic 15)

What Hypertext Transfer Protocol (HTTP) response header can be used to disable the execution of inline JavaScript and the execution of eval()-type functions?

- A. Strict-Transport-Security
- B. X-XSS-Protection
- C. X-Frame-Options
- D. Content-Security-Policy

**Answer:** D

#### NEW QUESTION 307

- (Exam Topic 15)

The security team has been tasked with performing an interface test against a frontend external facing application and needs to verify that all input fields protect against

invalid input. Which of the following BEST assists this process?

- A. Application fuzzing
- B. Instruction set simulation
- C. Regression testing
- D. Sanity testing

**Answer:** A

#### NEW QUESTION 312

- (Exam Topic 15)

In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

- A. Wide focus
- B. Strategic
- C. Anticipate
- D. Process

**Answer:** D

#### NEW QUESTION 317

- (Exam Topic 15)

Which of the (ISC)? Code of Ethics canons is MOST reflected when preserving the value of systems, applications, and entrusted information while avoiding conflicts of interest?

- A. Act honorably, honestly, justly, responsibly, and legally.
- B. Protect society, the commonwealth, and the infrastructure.
- C. Provide diligent and competent service to principles.
- D. Advance and protect the profession.

**Answer:** B

#### NEW QUESTION 320

- (Exam Topic 15)

What is the FIRST step in risk management?

- A. Establish the expectations of stakeholder involvement.
- B. Identify the factors that have potential to impact business.
- C. Establish the scope and actions required.
- D. Identify existing controls in the environment.

**Answer: C**

**NEW QUESTION 321**

- (Exam Topic 15)

Which of the following is a correct feature of a virtual local area network (VLAN)?

- A. A VLAN segregates network traffic therefore information security is enhanced significantly.
- B. Layer 3 routing is required to allow traffic from one VLAN to another.
- C. VLAN has certain security features such as where the devices are physically connected.
- D. There is no broadcast allowed within a single VLAN due to network segregation.

**Answer: A**

**NEW QUESTION 325**

- (Exam Topic 15)

Which of the following BEST describes why software assurance is critical in helping prevent an increase in business and mission risk for an organization?

- A. Software that does not perform as intended may be exploitable which makes it vulnerable to attack.
- B. Request for proposals (RFP) avoid purchasing software that does not meet business needs.
- C. Contracting processes eliminate liability for security vulnerabilities for the purchaser.
- D. Decommissioning of old software reduces long-term costs related to technical debt.

**Answer: B**

**NEW QUESTION 326**

- (Exam Topic 15)

An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

- A. Engage a third-party auditing firm.
- B. Review security architecture.
- C. Perform incremental assessments.
- D. Conduct penetration testing.

**Answer: C**

**NEW QUESTION 329**

- (Exam Topic 15)

Which of the following would be the BEST guideline to follow when attempting to avoid the exposure of sensitive data?

- A. Store sensitive data only when necessary.
- B. Educate end-users on methods of attacks on sensitive data.
- C. Establish report parameters for sensitive data.
- D. Monitor mail servers for sensitive data being exfiltrated.

**Answer: A**

**NEW QUESTION 332**

- (Exam Topic 15)

The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the foresight to enable what feature on all endpoints?

- A. Process isolation
- B. Trusted Platform Module (TPM)
- C. Address Space Layout Randomization (ASLR)
- D. Virtualization

**Answer: C**

**NEW QUESTION 333**

- (Exam Topic 15)

Which of the following are the three MAIN categories of security controls?

- A. Administrative, technical, physical
- B. Corrective, detective, recovery
- C. Confidentiality, integrity, availability
- D. Preventative, corrective, detective

**Answer: A**

**NEW QUESTION 335**

- (Exam Topic 15)

A company wants to implement two-factor authentication (2FA) to protect their computers from unauthorized users. Which solution provides the MOST secure means of authentication and meets the criteria they have set?



- A. Username and personal identification number (PIN)
- B. Fingerprint and retinal scanners
- C. Short Message Services (SMS) and smartphone authenticator
- D. Hardware token and password

**Answer:** D

#### NEW QUESTION 337

- (Exam Topic 15)

What action should be taken by a business line that is unwilling to accept the residual risk in a system after implementing compensating controls?

- A. Notify the audit committee of the situation.
- B. Purchase insurance to cover the residual risk.
- C. Implement operational safeguards.
- D. Find another business line willing to accept the residual risk.

**Answer:** B

#### NEW QUESTION 338

- (Exam Topic 15)

Which is the PRIMARY mechanism for providing the workforce with the information needed to protect an agency's vital information resources?

- A. Incorporating security awareness and training as part of the overall information security program
- B. An information technology (IT) security policy to preserve the confidentiality, integrity, and availability of systems
- C. Implementation of access provisioning process for coordinating the creation of user accounts
- D. Execution of periodic security and privacy assessments to the organization

**Answer:** A

#### NEW QUESTION 343

- (Exam Topic 15)

How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?

- A. Access control can rely on the Operating System (OS), but eavesdropping is
- B. Access control cannot rely on the Operating System (OS), and eavesdropping
- C. Access control can rely on the Operating System (OS), and eavesdropping is
- D. Access control cannot rely on the Operating System (OS), and eavesdropping

**Answer:** C

#### NEW QUESTION 347

- (Exam Topic 15)

A Chief Information Officer (CIO) has delegated responsibility of their system security to the head of the information technology (IT) department. While corporate policy dictates that only the CIO can make decisions on the level of data protection required, technical implementation decisions are done by the head of the IT department. Which of the following BEST describes the security role filled by the head of the IT department?

- A. System analyst
- B. System security officer
- C. System processor
- D. System custodian

**Answer:** D

#### NEW QUESTION 351

- (Exam Topic 15)

A software development company found odd behavior in some recently developed software, creating a need for a more thorough code review. What is the MOST effective argument for a more thorough code review?

- A. It will increase flexibility of the applications developed.
- B. It will increase accountability with the customers.
- C. It will impede the development process.
- D. It will reduce the potential for vulnerabilities.

**Answer:** D

#### NEW QUESTION 353

- (Exam Topic 15)

When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

- A. Requirements
- B. Risk assessment
- C. Due diligence
- D. Planning

**Answer:** B

#### NEW QUESTION 357

- (Exam Topic 15)

Which of the following is the MOST important first step in preparing for a security audit?

- A. Identify team members.
- B. Define the scope.
- C. Notify system administrators.
- D. Collect evidence.

**Answer: B**

#### NEW QUESTION 358

- (Exam Topic 15)

Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

- A. Control traffic
- B. Prevent rapid movement
- C. Prevent plggybacking
- D. Control air flow

**Answer: C**

#### NEW QUESTION 359

- (Exam Topic 15)

A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS).

Which of the following factors leads the company to choose an IDaaS as their solution?

- A. In-house development provides more control.
- B. In-house team lacks resources to support an on-premise solution.
- C. Third-party solutions are inherently more secure.
- D. Third-party solutions are known for transferring the risk to the vendor.

**Answer: B**

#### NEW QUESTION 361

- (Exam Topic 15)

Which of the following encryption technologies has the ability to function as a stream cipher?

- A. Cipher Feedback (CFB)
- B. Feistel cipher
- C. Cipher Block Chaining (CBC) with error propagation
- D. Electronic Code Book (ECB)

**Answer: A**

#### NEW QUESTION 365

- (Exam Topic 15)

Which evidence collecting technique would be utilized when it is believed an attacker is employing a rootkit and a quick analysis is needed?

- A. Memory collection
- B. Forensic disk imaging
- C. Malware analysis
- D. Live response

**Answer: A**

#### NEW QUESTION 366

- (Exam Topic 15)

The adoption of an enterprise-wide Business Continuity (BC) program requires which of the following?

- A. Good communication throughout the organization
- B. A completed Business Impact Analysis (BIA)
- C. Formation of Disaster Recovery (DR) project team
- D. Well-documented information asset classification

**Answer: D**

#### NEW QUESTION 370

- (Exam Topic 15)

An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

- A. Cross-Site Scripting (XSS)
- B. Pass the ticket
- C. Brute force



D. Hash collision

**Answer:** B

#### NEW QUESTION 371

- (Exam Topic 15)

Of the following, which BEST provides non- repudiation with regards to access to a server room?

- A. Fob and Personal Identification Number (PIN)
- B. Locked and secured cages
- C. Biometric readers
- D. Proximity readers

**Answer:** C

#### NEW QUESTION 374

- (Exam Topic 15)

A web-based application known to be susceptible to attacks is now under review by a senior developer. The organization would like to ensure this application is less susceptible to injection attacks specifically, What strategy will work BEST for the organization's situation?

- A. Do not store sensitive unencrypted data on the back end.
- B. Whitelist input and encode or escape output before it is processed for rendering.
- C. Limit privileged access or hard-coding logon credentials,
- D. Store sensitive data in a buffer that retains data in operating system (OS) cache or memory.

**Answer:** B

#### NEW QUESTION 378

- (Exam Topic 15)

Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

- A. Audit
- B. Compliance
- C. Legal
- D. Security

**Answer:** C

#### NEW QUESTION 379

- (Exam Topic 15)

When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

- A. The actual origin and tools used for the test can be hidden.
- B. Information may be found on related breaches and hacking.
- C. Vulnerabilities can be tested without impact on the tested environment.
- D. Information may be found on hidden vendor patches.

**Answer:** D

#### NEW QUESTION 384

- (Exam Topic 15)

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

- A. nslookup
- B. netstat -a
- C. ipconfig /a
- D. arp -a

**Answer:** B

#### NEW QUESTION 386

- (Exam Topic 15)

A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

- A. Federation authorities
- B. Proxied federation
- C. Static registration
- D. Dynamic registration

**Answer:** D

#### NEW QUESTION 391

- (Exam Topic 15)

Which of the following BEST ensures the integrity of transactions to intended recipients?

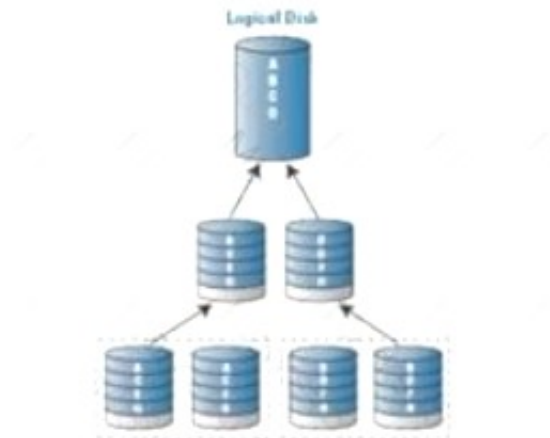
- A. Public key infrastructure (PKI)
- B. Blockchain technology
- C. Pre-shared key (PSK)
- D. Web of trust

**Answer: A**

#### NEW QUESTION 393

- (Exam Topic 15)

Which Redundant Array c/ Independent Disks (RAID) Level does the following diagram represent?



- A. RAID 0
- B. RAID 1
- C. RAID 5
- D. RAID 10

**Answer: D**

#### NEW QUESTION 395

- (Exam Topic 15)

Which of the following is the BEST option to reduce the network attack surface of a system?

- A. Ensuring that there are no group accounts on the system
- B. Removing unnecessary system user accounts
- C. Disabling unnecessary ports and services
- D. Uninstalling default software on the system

**Answer: C**

#### NEW QUESTION 397

- (Exam Topic 15)

What is the PRIMARY objective of business continuity planning?

- A. Establishing a cost estimate for business continuity recovery operations
- B. Restoring computer systems to normal operations as soon as possible
- C. Strengthening the perceived importance of business continuity planning among senior management
- D. Ensuring timely recovery of mission-critical business processes

**Answer: B**

#### NEW QUESTION 398

- (Exam Topic 15)

a large organization uses biometrics to allow access to its facilities. It adjusts the biometric value for incorrectly granting or denying access so that the two numbers are the same.

What is this value called?

- A. False Rejection Rate (FRR)
- B. Accuracy acceptance threshold
- C. Equal error rate
- D. False Acceptance Rate (FAR)

**Answer: C**

#### NEW QUESTION 403

- (Exam Topic 15)

An organization is preparing to achieve General Data Protection Regulation (GDPR) compliance. The Chief Information Security Officer (CISO) is reviewing data protection methods.

Which of the following is the BEST data protection method?

- A. Encryption

- B. Backups
- C. Data obfuscation
- D. Strong authentication

**Answer:** C

#### NEW QUESTION 407

- (Exam Topic 15)

When performing an investigation with the potential for legal action, what should be the analyst's FIRST consideration?

- A. Chain-of-custody
- B. Authorization to collect
- C. Court admissibility
- D. Data decryption

**Answer:** A

#### NEW QUESTION 412

- (Exam Topic 15)

An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

- A. 1
- B. 2
- C. 3

**Answer:** A

#### NEW QUESTION 415

- (Exam Topic 15)

An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

- A. nslookup
- B. show config
- C. netstat
- D. show interface
- E. show counters

**Answer:** D

#### NEW QUESTION 419

- (Exam Topic 15)

Write Once, Read Many (WORM) data storage devices are designed to BEST support which of the following core security concepts?

- A. Integrity
- B. Scalability
- C. Availability
- D. Confidentiality

**Answer:** A

#### NEW QUESTION 424

- (Exam Topic 15)

Which software defined networking (SDN) architectural component is responsible for translating network requirements?

- A. SDN Application
- B. SDN Data path
- C. SDN Controller
- D. SDN Northbound Interfaces

**Answer:** D

#### NEW QUESTION 429

- (Exam Topic 15)

A large manufacturing organization arranges to buy an industrial machine system to produce a new line of products. The system includes software provided to the vendor by a thirdparty organization. The financial risk to the manufacturing organization starting production is high. What step should the manufacturing organization take to minimize its financial risk in the new venture prior to the purchase?

- A. Hire a performance tester to execute offline tests on a system.
- B. Calculate the possible loss in revenue to the organization due to software bugs and vulnerabilities, and compare that to the system's overall price.
- C. Place the machine behind a Layer 3 firewall.
- D. Require that the software be thoroughly tested by an accredited independent software testing company.

**Answer:** B

#### NEW QUESTION 430

- (Exam Topic 15)

What is the BEST method to use for assessing the security impact of acquired software?

- A. Common vulnerability review
- B. Software security compliance validation
- C. Threat modeling
- D. Vendor assessment

**Answer:** B

#### NEW QUESTION 434

- (Exam Topic 15)

Which of the following BEST describes the standard used to exchange authorization information between different identity management systems?

- A. Security Assertion Markup Language (SAML)
- B. Service Oriented Architecture (SOA)
- C. Extensible Markup Language (XML)
- D. Wireless Authentication Protocol (WAP)

**Answer:** A

#### NEW QUESTION 436

- (Exam Topic 15)

What is the MOST common security risk of a mobile device?

- A. Insecure communications link
- B. Data leakage
- C. Malware infection
- D. Data spoofing

**Answer:** C

#### NEW QUESTION 440

- (Exam Topic 15)

An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization's dedicated environment with a cloud service provider. What is the BEST way to prevent and correct the software's security weakness?

- A. Implement a dedicated COTS sandbox environment
- B. Follow the software end-of-life schedule
- C. Transfer the risk to the cloud service provider
- D. Examine the software updating and patching process

**Answer:** A

#### NEW QUESTION 443

- (Exam Topic 15)

The MAIN purpose of placing a tamper seal on a computer system's case is to:

- A. raise security awareness.
- B. detect efforts to open the case.
- C. expedite physical auditing.
- D. make it difficult to steal internal components.

**Answer:** A

#### NEW QUESTION 446

- (Exam Topic 15)

International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

- A. General Data Protection Regulation (GDPR)
- B. Palermo convention
- C. Wassenaar arrangement
- D. International Traffic in Arms Regulations (ITAR)

**Answer:** C

#### NEW QUESTION 448

- (Exam Topic 15)

The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

- A. Skill set and training
- B. Headcount and capacity
- C. Tools and technologies

D. Scope and service catalog

**Answer: C**

#### NEW QUESTION 449

- (Exam Topic 15)

A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

- A. Validate passwords using a stored procedure.
- B. Allow only the application to have access to the password field in order to verify user authentication.
- C. Use a salted cryptographic hash of the password.
- D. Encrypt the entire database and embed an encryption key in the application.

**Answer: C**

#### NEW QUESTION 453

- (Exam Topic 15)

How should the retention period for an organization's social media content be defined?

- A. By the retention policies of each social media service
- B. By the records retention policy of the organization
- C. By the Chief Information Officer (CIO)
- D. By the amount of available storage space

**Answer: B**

#### NEW QUESTION 456

- (Exam Topic 15)

If traveling abroad and a customs official demands to examine a personal computer, which of the following should be assumed?

- A. The hard drive has been stolen.
- B. The Internet Protocol (IP) address has been copied.
- C. The hard drive has been copied.
- D. The Media Access Control (MAC) address was stolen

**Answer: C**

#### NEW QUESTION 459

- (Exam Topic 15)

While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

- A. Detective and recovery controls
- B. Corrective and recovery controls
- C. Preventative and corrective controls
- D. Recovery and proactive controls

**Answer: C**

#### NEW QUESTION 463

- (Exam Topic 15)

In what phase of the System Development Life Cycle (SDLC) should security training for the development team begin?

- A. Development/Acquisition
- B. Initiation
- C. Implementation/ Assessment
- D. Disposal

**Answer: A**

#### NEW QUESTION 466

- (Exam Topic 15)

A manager identified two conflicting sensitive user functions that were assigned to a single user account that had the potential to result in financial and regulatory risk to the company. The manager MOST likely discovered this during which of the following?

- A. Security control assessment.
- B. Separation of duties analysis
- C. Network Access Control (NAC) review
- D. Federated identity management (FIM) evaluation

**Answer: B**

#### NEW QUESTION 469

- (Exam Topic 15)

A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?

- A. Upgrade the software affected by the vulnerability.
- B. Inform management of possible risks.
- C. Mitigate the risks with compensating controls.
- D. Remove the affected software from the servers.

**Answer:** C

#### NEW QUESTION 472

- (Exam Topic 15)

A firm within the defense industry has been directed to comply with contractual requirements for encryption of a government client's Controlled Unclassified Information (CUI). What encryption strategy represents how to protect data at rest in the MOST efficient and cost-effective manner?

- A. Perform physical separation of program information and encrypt only information deemed critical by the defense client
- B. Perform logical separation of program information, using virtualized storage solutions with built-in encryption at the virtualization layer
- C. Perform logical separation of program information, using virtualized storage solutions with encryption management in the back-end disk systems
- D. Implement data at rest encryption across the entire storage area network (SAN)

**Answer:** C

#### NEW QUESTION 476

- (Exam Topic 15)

Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

- A. Training
- B. Legal
- C. Business
- D. Storage

**Answer:** B

#### NEW QUESTION 480

- (Exam Topic 15)

Which of the following is the FIRST step during digital identity provisioning?

- A. Authorizing the entity for resource access
- B. Synchronizing directories
- C. Issuing an initial random password
- D. Creating the entity record with the correct attributes

**Answer:** D

#### NEW QUESTION 483

- (Exam Topic 15)

To monitor the security of buried data lines inside the perimeter of a facility, which of the following is the MOST effective control?

- A. Fencing around the facility with closed-circuit television (CCTV) cameras at all entry points
- B. Ground sensors installed and reporting to a security event management (SEM) system
- C. Steel casing around the facility ingress points
- D. regular sweeps of the perimeter, including manual inspection of the cable ingress points

**Answer:** D

#### NEW QUESTION 487

- (Exam Topic 15)

Why are packet filtering routers used in low-risk environments?

- A. They are high-resolution source discrimination and identification tools.
- B. They are fast and flexible, and protect against Internet Protocol (IP) spoofing.
- C. They are fast, flexible, and transparent.
- D. They enforce strong user authentication and audit log generation.

**Answer:** B

#### NEW QUESTION 490

- (Exam Topic 15)

The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery. Which of the following is the MOST challenging aspect of this investigation?

- A. SCADA network latency
- B. Group policy implementation
- C. Volatility of data
- D. Physical access to the system

**Answer:** C



#### NEW QUESTION 493

- (Exam Topic 15)

A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging generates extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

- A. Keep last week's logs in an online storage and the rest in a near-line storage.
- B. Keep all logs in an online storage.
- C. Keep all logs in an offline storage.
- D. Keep last week's logs in an online storage and the rest in an offline storage.

**Answer: D**

#### NEW QUESTION 494

- (Exam Topic 15)

All hosts on the network are sending logs via syslog-ng to the log collector. The log collector is behind its own firewall, The security professional wants to make sure not to put extra load on the firewall due to the amount of traffic that is passing through it. Which of the following types of filtering would MOST likely be used?

- A. Uniform Resource Locator (URL) Filtering
- B. Web Traffic Filtering
- C. Dynamic Packet Filtering
- D. Static Packet Filtering

**Answer: C**

#### NEW QUESTION 495

- (Exam Topic 15)

What is the overall goal of software security testing?

- A. Identifying the key security features of the software
- B. Ensuring all software functions perform as specified
- C. Reducing vulnerabilities within a software system
- D. Making software development more agile

**Answer: B**

#### NEW QUESTION 498

- (Exam Topic 15)

Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

- A. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools
- B. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools
- C. Maintaining the inventory through a combination of on-premise storage configuration, cloud management, and partner management tools
- D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

**Answer: C**

#### NEW QUESTION 501

- (Exam Topic 15)

What is the PRIMARY reason that a bit-level copy is more desirable than a file-level copy when replicating a hard drive's contents for an e-discovery investigation?

- A. Files that have been deleted will be transferred.
- B. The file and directory structure is retained.
- C. File-level security settings will be preserved.
- D. The corruption of files is less likely.

**Answer: A**

#### NEW QUESTION 502

- (Exam Topic 15)

What is the FIRST step prior to executing a test of an organisation's disaster recovery (DR) or business continuity plan (BCP)?

- A. identify key stakeholders,
- B. Develop recommendations for disaster scenarios.
- C. Identify potential failure points.
- D. Develop clear evaluation criteria.

**Answer: D**

#### NEW QUESTION 507

- (Exam Topic 15)

The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a particular system over a 12-month period. Which type of SOC report should be utilized?

- A. SOC 1 Type 1
- B. SOC 2 Type 2



- C. SOC 2 Type 2
- D. SOC 3 Type 1

**Answer:** C

**NEW QUESTION 508**

- (Exam Topic 15)

employee training, risk management, and data handling procedures and policies could be characterized as which type of security measure?

- A. Non-essential
- B. Management
- C. Preventative
- D. Administrative

**Answer:** D

**NEW QUESTION 511**

- (Exam Topic 15)

What is the BEST design for securing physical perimeter protection?

- A. Crime Prevention through Environmental Design (CPTED)
- B. Barriers, fences, gates, and walls
- C. Business continuity planning (BCP)
- D. Closed-circuit television (CCTV)

**Answer:** B

**NEW QUESTION 512**

- (Exam Topic 15)

Which of the following BEST describes when an organization should conduct a black box security audit on a new software product?

- A. When the organization wishes to check for non-functional compliance
- B. When the organization wants to enumerate known security vulnerabilities across their infrastructure
- C. When the organization has experienced a security incident
- D. When the organization is confident the final source code is complete

**Answer:** B

**NEW QUESTION 516**

- (Exam Topic 15)

When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

- A. Resiliency of the system
- B. Detection of sophisticated attackers
- C. Risk assessment of the system
- D. Topology of the network used for the system

**Answer:** A

**NEW QUESTION 521**

- (Exam Topic 15)

Which of the following VPN configurations should be used to separate Internet and corporate traffic?

- A. Split-tunnel
- B. Remote desktop gateway
- C. Site-to-site
- D. Out-of-band management

**Answer:** A

**NEW QUESTION 522**

- (Exam Topic 15)

A security professional is assessing the risk in an application and does not take into account any mitigating or compensating controls. This type of risk rating is an example of which of the following?

- A. Transferred risk
- B. Inherent risk
- C. Residual risk
- D. Avoided risk

**Answer:** B

**NEW QUESTION 524**

- (Exam Topic 15)

Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

- A. Centralized network provisioning
- B. Centralized network administrator control
- C. Reduced network latency when scaled
- D. Reduced hardware footprint and cost

**Answer:** B

#### NEW QUESTION 527

- (Exam Topic 15)

Which of the following is used to ensure that data mining activities Will NOT reveal sensitive data?

- A. Implement two-factor authentication on the underlying infrastructure.
- B. Encrypt data at the field level and tightly control encryption keys.
- C. Preprocess the databases to see if inn ..... can be disclosed from the learned patterns.
- D. Implement the principle of least privilege on data elements so a reduced number of users can access the database.

**Answer:** D

#### NEW QUESTION 532

- (Exam Topic 15)

Which of the following protection is provided when using a Virtual Private Network (VPN) with Authentication Header (AH)?

- A. Payload encryption
- B. Sender confidentiality
- C. Sender non-repudiation
- D. Multi-factor authentication (MFA)

**Answer:** C

#### NEW QUESTION 537

- (Exam Topic 15)

An organization outgrew its internal data center and is evaluating third-party hosting facilities. In this evaluation, which of the following is a PRIMARY factor for selection?

- A. Facility provides an acceptable level of risk
- B. Facility provides disaster recovery (DR) services
- C. Facility provides the most cost-effective solution
- D. Facility has physical access protection measures

**Answer:** C

#### NEW QUESTION 539

- (Exam Topic 15)

A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to on and security However, an attacker was able to spoof a registered account on the network and query the SAML provider.

What is the MOST common attack leverage against this flaw?

- A. Attacker forges requests to authenticate as a different user.
- B. Attacker leverages SAML assertion to register an account on the security domain.
- C. Attacker conducts denial-of-service (DoS) against the security domain by authenticating as the same user repeatedly.
- D. Attacker exchanges authentication and authorization data between security domains.

**Answer:** A

#### NEW QUESTION 540

- (Exam Topic 15)

Which of the following BEST describes centralized identity management?

- A. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
- B. Service providers agree to integrate identity system recognition across organizational boundaries.
- C. Service providers identify an entity by behavior analysis versus an identification factor.
- D. Service providers perform as both the credential and identity provider (IdP).

**Answer:** B

#### NEW QUESTION 543

- (Exam Topic 15)

How is it possible to extract private keys securely stored on a cryptographic smartcard?

- A. Bluebugging
- B. Focused ion-beam
- C. Bluejacking
- D. Power analysis

**Answer:** D

#### NEW QUESTION 545

- (Exam Topic 15)

The security architect has been mandated to assess the security of various brands of mobile devices. At what phase of the product lifecycle would this be MOST likely to occur?

- A. Disposal
- B. Implementation
- C. Development
- D. Operations and maintenance

**Answer: C**

#### NEW QUESTION 547

- (Exam Topic 15)

Which of the following is a covert channel type?

- A. Storage
- B. Pipe
- C. Memory
- D. Monitoring

**Answer: A**

#### NEW QUESTION 550

- (Exam Topic 15)

Which of the following is a standard Access Control List (ACL) element that enables a router to filter Internet traffic?

- A. Media Access Control (MAC) address
- B. Internet Protocol (IP) address
- C. Security roles
- D. Device needs

**Answer: B**

#### NEW QUESTION 551

- (Exam Topic 15)

In which of the following scenarios is locking server cabinets and limiting access to keys preferable to locking the server room to prevent unauthorized access?

- A. Server cabinets are located in an unshared workspace.
- B. Server cabinets are located in an isolated server farm.
- C. Server hardware is located in a remote area.
- D. Server cabinets share workspace with multiple projects.

**Answer: D**

#### NEW QUESTION 556

- (Exam Topic 15)

When are security requirements the LEAST expensive to implement?

- A. When identified by external consultants
- B. During the application rollout phase
- C. During each phase of the project cycle
- D. When built into application design

**Answer: D**

#### NEW QUESTION 558

- (Exam Topic 15)

A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

- A. Network is flooded with communication traffic by the attacker.
- B. Organization loses control of their network devices.
- C. Network management communications is disrupted.
- D. Attacker accesses sensitive information regarding the network topology.

**Answer: B**

#### NEW QUESTION 560

- (Exam Topic 15)

An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

- A. Hybrid
- B. Federated
- C. Decentralized
- D. Centralized

**Answer:** A

**NEW QUESTION 561**

- (Exam Topic 15)

In Federated Identity Management (FIM), which of the following represents the concept of federation?

- A. Collection of information logically grouped into a single entity
- B. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications
- C. Collection of information for common identities in a system
- D. Collection of domains that have established trust among themselves

**Answer:** D

**NEW QUESTION 563**

- (Exam Topic 15)

An organization contracts with a consultant to perform a System Organization Control (SOC) 2 audit on their internal security controls. An auditor documents a finding related to an Application Programming Interface (API) performing an action that is not aligned with the scope or objective of the system. Which trust service principle would be MOST applicable in this situation?

- A. Processing Integrity
- B. Availability
- C. Confidentiality
- D. Security

**Answer:** B

**NEW QUESTION 564**

- (Exam Topic 15)

What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

- A. Implement egress filtering at the organization's network boundary.
- B. Implement network access control lists (ACL).
- C. Implement a web application firewall (WAF).
- D. Implement an intrusion prevention system (IPS).

**Answer:** B

**NEW QUESTION 567**

- (Exam Topic 15)

The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

- A. Data masking and encryption of personal data
- B. Only to use encryption protocols approved by EU
- C. Anonymization of personal data when transmitted to sources outside the EU
- D. Never to store personal data of EU citizens outside the EU

**Answer:** D

**NEW QUESTION 571**

- (Exam Topic 15)

When MUST an organization's information security strategic plan be reviewed?

- A. Quarterly, when the organization's strategic plan is updated
- B. Whenever there are significant changes to a major application
- C. Every three years, when the organization's strategic plan is updated
- D. Whenever there are major changes to the business

**Answer:** D

**NEW QUESTION 572**

- (Exam Topic 15)

What should be used to determine the risks associated with using Software as a Service (SaaS) for collaboration and email?

- A. Cloud access security broker (CASB)
- B. Open Web Application Security Project (OWASP)
- C. Process for Attack Simulation and Threat Analysis (PASTA)
- D. Common Security Framework (CSF)

**Answer:** A

**NEW QUESTION 576**

- (Exam Topic 15)

How should the retention period for an organization's social media content be defined?

- A. Wireless Access Points (AP)
- B. Token-based authentication
- C. Host-based firewalls
- D. Trusted platforms

**Answer:** C

#### NEW QUESTION 577

- (Exam Topic 15)

The initial security categorization should be done early in the system life cycle and should be reviewed periodically. Why is it important for this to be done correctly?

- A. It determines the security requirements.
- B. It affects other steps in the certification and accreditation process.
- C. It determines the functional and operational requirements.
- D. The system engineering process works with selected security controls.

**Answer:** B

#### NEW QUESTION 581

- (Exam Topic 15)

A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should be an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

- A. SOC 1
- B. SOC 2 Type I
- C. SOC 2 Type II
- D. SOC 3

**Answer:** D

#### NEW QUESTION 585

- (Exam Topic 15)

Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

- A. Distributed denial-of-service (DDoS) attack
- B. Zero-day attack
- C. Phishing attempt
- D. Advanced persistent threat (APT) attempt

**Answer:** A

#### NEW QUESTION 586

- (Exam Topic 15)

In an IDEAL encryption system, who has sole access to the decryption key?

- A. System owner
- B. Data owner
- C. Data custodian
- D. System administrator

**Answer:** B

#### NEW QUESTION 588

- (Exam Topic 15)

A retail company is looking to start a development project that will utilize open source components in its code for the first time. The development team has already acquired several 'open source components and utilized them in proof of concept (POC) code. The team recognizes that the legal and operational risks are outweighed by the benefits of open-source software use. What MUST the organization do next?

- A. Mandate that all open-source components be approved by the Information Security Manager (ISM).
- B. Scan all open-source components for security vulnerabilities.
- C. Establish an open-source compliance policy.
- D. Require commercial support for all open-source components.

**Answer:** C

#### NEW QUESTION 593

- (Exam Topic 15)

The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

- A. biometric data cannot be changed.
- B. Separate biometric data streams require increased security.
- C. The biometric devices are unknown.
- D. Biometric data must be protected from disclosure.

**Answer:** A

#### NEW QUESTION 596

- (Exam Topic 15)

Which of the following system components enforces access controls on an object?

- A. Security perimeter
- B. Access control matrix
- C. Trusted domain
- D. Reference monitor

**Answer: B**

#### NEW QUESTION 599

- (Exam Topic 15)

Which of the following BEST describes botnets?

- A. Computer systems on the Internet that are set up to trap people who attempt to penetrate other computer system
- B. Set of related programs that protects the resources of a private network from other networks
- C. Small network inserted in a neutral zone between an organization's private network and the outside public network
- D. Groups of computers that are used to launch destructive attacks

**Answer: D**

#### NEW QUESTION 600

- (Exam Topic 15)

Building blocks for software-defined networks (SDN) require which of the following?

- A. The SDN is mostly composed of virtual machines (VM).
- B. The SDN is composed entirely of client-server pairs.
- C. Virtual memory is used in preference to random-access memory (RAM).
- D. Random-access memory (RAM) is used in preference to virtual memory.

**Answer: C**

#### NEW QUESTION 602

- (Exam Topic 14)

What form of attack could this represent?

- A. A Denial of Service (DoS) attack against the gateway router because the router can no longer accept packets from
- B. A transport layer attack that prevents the resolution of 10.102.10.6 address
- C. A Denial of Service (DoS) attack against 10.102.10.2 because it cannot respond correctly to ARP requests
- D. A masquerading attack that sends packets intended for 10.102.10.6 to 10.102.10.2

**Answer: D**

#### NEW QUESTION 605

- (Exam Topic 14)

Which of the following are core categories of malicious attack against Internet of Things (IOT) devices?

- A. Packet capture and false data injection
- B. Packet capture and brute force attack
- C. Node capture 3rd Structured Query Language (SQL) injection
- D. Node capture and false data injection

**Answer: D**

#### NEW QUESTION 609

- (Exam Topic 14)

In a dispersed network that lacks central control, which of the following is die PRIMARY course of action to mitigate exposure?

- A. Implement management policies, audit control, and data backups
- B. Implement security policies and standards, access controls, and access limitations
- C. Implement security policies and standards, data backups, and audit controls
- D. Implement remote access policies, shared workstations, and log management

**Answer: C**

#### NEW QUESTION 611

- (Exam Topic 14)

Which one of the following documentation should be included in a Disaster Recovery (DR) package?

- A. Source code, compiled code, firmware updates, operational log book and manuals.
- B. Data encrypted in original format, auditable transaction data, and recovery instructions for future extraction on demand.
- C. Hardware configuration instructions, hardware configuration software, an operating system image, a data restoration option, media retrieval instructions,.....
- D. System configuration including hardware, software, hardware, interfaces, software Application Programming Interface (API) configuration, data structure, ....

**Answer:**



C

#### NEW QUESTION 616

- (Exam Topic 14)

Which of the following entails identification of data end links to business processes, applications, and data stores as well as assignment of ownership responsibilities?

- A. Risk management
- B. Security portfolio management
- C. Security governance
- D. Risk assessment

**Answer: A**

#### NEW QUESTION 618

- (Exam Topic 14)

What should an auditor do when conducting a periodic audit on media retention?

- A. Check electronic storage media to ensure records are not retained past their destruction date.
- B. Ensure authorized personnel are in possession of paper copies containing Personally Identifiable Information....
- C. Check that hard disks containing backup data that are still within a retention cycle are being destroyed....
- D. Ensure that data shared with outside organizations is no longer on a retention schedule.

**Answer: A**

#### NEW QUESTION 621

- (Exam Topic 14)

Which of the following is TRUE regarding equivalence class testing?

- A. It is characterized by the stateless behavior of a process implemented In a function.
- B. An entire partition can be covered by considering only one representative value from that partition.
- C. Test inputs are obtained from the derived boundaries of the given functional specifications.
- D. It is useful for testing communications protocols and graphical user interfaces.

**Answer: C**

#### NEW QUESTION 625

- (Exam Topic 14)

Activity to baseline, tailor, and scope security controls takes place during which National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) step?

- A. Authorize IS.
- B. Assess security controls.
- C. Categorize Information system (IS).
- D. Select security controls.

**Answer: D**

#### NEW QUESTION 627

- (Exam Topic 14)

What protocol is often used between gateway hosts on the Internet? To control the scope of a Business Continuity Management (BCM) system, a security practitioner should identify which of the following?

- A. Size, nature, and complexity of the organization
- B. Business needs of the security organization
- C. All possible risks
- D. Adaptation model for future recovery planning

**Answer: B**

#### NEW QUESTION 628

- (Exam Topic 14)

An organization wants to enable users to authenticate across multiple security domains. To accomplish this they have decided to use Federated Identity Management (FIM). Which of the following is used behind the scenes in a FIM deployment?

- A. Standard Generalized Markup Language (SGML)
- B. Extensible Markup Language (XML)
- C. Security Assertion Markup Language (SAML)
- D. Transaction Authority Markup Language (XAML)

**Answer: C**

#### NEW QUESTION 633

- (Exam Topic 14)

An organization has implemented a new backup process which protects confidential data by encrypting the information stored on backup tapes. Which of the following is a MAJOR data confidentiality concern after the implementation of this new backup process?



- A. Tape backup rotation
- B. Pre-existing backup tapes
- C. Tape backup compression
- D. Backup tape storage location

**Answer:** D

#### NEW QUESTION 637

- (Exam Topic 14)

Why should Open Web Application Security Project (OWASP) Application Security Verification standards (ASVS) Level 1 be considered a MINIMUM level of protection for any web application?

- A. ASVS Level 1 ensures that applications are invulnerable to OWASP top 10 threats.
- B. Opportunistic attackers will look for any easily exploitable vulnerable applications.
- C. Most regulatory bodies consider ASVS Level 1 as a baseline set of controls for applications.
- D. Securing applications at ASVS Level 1 provides adequate protection for sensitive data.

**Answer:** B

#### NEW QUESTION 641

- (Exam Topic 14)

Internet protocol security (IPSec), point-to-point tunneling protocol (PPTP), and secure sockets Layer (SSL) all use Which of the following to prevent replay attacks?

- A. Large Key encryption
- B. Single integrity protection
- C. Embedded sequence numbers
- D. Randomly generated nonces

**Answer:** C

#### NEW QUESTION 642

- (Exam Topic 14)

If a content management system (CMC) is implemented, which one of the following would occur?

- A. Developers would no longer have access to production systems
- B. The applications placed into production would be secure
- C. Patching the systems would be completed more quickly
- D. The test and production systems would be running the same software

**Answer:** D

#### NEW QUESTION 646

- (Exam Topic 14)

How long should the records on a project be retained?

- A. For the duration of the project, or at the discretion of the record owner
- B. Until they are no longer useful or required by policy
- C. Until five years after the project ends, then move to archives
- D. For the duration of the organization fiscal year

**Answer:** B

#### NEW QUESTION 647

- (Exam Topic 14)

What access control scheme uses fine-grained rules to specify the conditions under which access to each data item or applications is granted?

- A. Mandatory Access Control (MAC)
- B. Discretionary Access Control (DAC)
- C. Role Based Access Control (RBAC)
- D. Attribute Based Access Control (ABAC)

**Answer:** D

#### Explanation:

Reference: [https://en.wikipedia.org/wiki/Attribute-based\\_access\\_control](https://en.wikipedia.org/wiki/Attribute-based_access_control)

#### NEW QUESTION 651

- (Exam Topic 14)

Functional security testing is MOST critical during which phase of the system development life cycle (SDLC)?

- A. Operations / Maintenance
- B. Implementation
- C. Acquisition / Development
- D. Initiation

**Answer:**

B

#### NEW QUESTION 654

- (Exam Topic 14)

- A. Verify the camera's log for recent logins outside of the Internet Technology (IT) department.
- B. Verify the security and encryption protocol the camera uses.
- C. Verify the security camera requires authentication to log into the management console.
- D. Verify the most recent firmware version is installed on the camera.

**Answer:** D

#### NEW QUESTION 655

- (Exam Topic 14)

Compared with hardware cryptography, software cryptography is generally

- A. less expensive and slower.
- B. more expensive and faster.
- C. more expensive and slower.
- D. less expensive and faster.

**Answer:** A

#### Explanation:

Reference:

<https://www.ontrack.com/uk/blog/making-data-simple/hardware-encryption-vs-software-encryption-the-simple>

#### NEW QUESTION 659

- (Exam Topic 14)

How can an attacker exploit overflow to execute arbitrary code?

- A. Modify a function's return address.
- B. Alter the address of the stack.
- C. Substitute elements in the stack.
- D. Move the stack pointer.

**Answer:** A

#### NEW QUESTION 661

- (Exam Topic 14)

Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

- A. Process isolation
- B. Data hiding and abstraction
- C. Use of discrete layering and Application Programming Interfaces (API)
- D. Virtual Private Network (VPN)

**Answer:** C

#### Explanation:

Reference: <https://books.google.com.pk/books?id=LnjxBwAAQBAJ&pg=PT504&lpg=PT504&dq=CISSP+mechanism+us>

#### NEW QUESTION 664

- (Exam Topic 14)

Which is the MOST critical aspect of computer-generated evidence?

- A. Objectivity
- B. Integrity
- C. Timeliness
- D. Relevancy

**Answer:** B

#### NEW QUESTION 665

- (Exam Topic 14)

Which of the following is a method of attacking internet (IP) v6 Layer 3 and Layer 4 ?

- A. Synchronize sequence numbers (SVN) flooding
- B. Internet Control Message Protocol (IOP) flooring
- C. Domain Name Server (DNS) cache poisoning
- D. Media Access Control (MAC) flooding

**Answer:** A

#### NEW QUESTION 668

- (Exam Topic 14)

An organization has a short-term agreement with a public Cloud Service Provider (CSP). Which of the following BEST protects sensitive data once the agreement expires and the assets are reused?

- A. Recommended that the business data owners use continuous monitoring and analysis of applications to prevent data loss.
- B. Recommend that the business data owners use internal encryption keys for data-at-rest and data-in-transit to the storage environment.
- C. Use a contractual agreement to ensure the CSP wipes the data from the storage environment.
- D. Use a National Institute of Standards and Technology (NIST) recommendation for wiping data on the storage environment.

**Answer:** C

#### NEW QUESTION 673

- (Exam Topic 14)

Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

- A. An attack which forces an end user to execute unwanted actions on a web application in which they are currently authenticated
- B. An attack that injects a script into a web page to execute a privileged command
- C. An attack that makes an illegal request across security zones and thereby forges itself into the security database of the system
- D. An attack that forges a false Structure Query Language (SQL) command across systems

**Answer:** A

#### Explanation:

Reference: <https://portswigger.net/web-security/csrf>

#### NEW QUESTION 676

- (Exam Topic 14)

What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

- A. Manual inspections and reviews
- B. Penetration testing
- C. Threat modeling
- D. Source code review

**Answer:** C

#### NEW QUESTION 681

- (Exam Topic 14)

When dealing with shared, privileged accounts, especially those for emergencies, what is the BEST way to assure non-repudiation of logs?

- A. Regularly change the passwords,
- B. implement a password vaulting solution.
- C. Lock passwords in tamperproof envelopes in a safe.
- D. Implement a strict access control policy.

**Answer:** B

#### NEW QUESTION 684

- (Exam Topic 14)

When should an application invoke re-authentication in addition to initial user authentication?

- A. At the application sign-off
- B. Periodically during a session
- C. After a period of inactivity
- D. For each business process

**Answer:** C

#### NEW QUESTION 685

- (Exam Topic 14)

Which of the following is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services?

- A. The acquiring organization
- B. The service provider
- C. The risk executive (function)
- D. The IT manager

**Answer:** C

#### NEW QUESTION 687

- (Exam Topic 14)

Which of the following is the final phase of the identity and access provisioning lifecycle?

- A. Recertification
- B. Revocation
- C. Removal

D. Validation

**Answer:** B

**Explanation:**

Reference: <https://books.google.com.pk/books?id=W2TvAgAAQBAJ&pg=PA256&lpg=PA256&dq=process+in+the+acce>

#### NEW QUESTION 688

- (Exam Topic 14)

An organization discovers that its secure file transfer protocol (SFTP) server has been accessed by an unauthorized person to download an unreleased game. A recent security audit found weaknesses in some of the organization's general information technology (IT) controls, specifically pertaining to software change control and security patch management, but not in other control areas.

Which of the following is the MOST probable attack vector used in the security breach?

- A. Buffer overflow
- B. Weak password able to lack of complexity rules
- C. Distributed Denial of Service (DDoS)
- D. Cross-Site Scripting (XSS)

**Answer:** A

#### NEW QUESTION 693

- (Exam Topic 14)

Who determines the required level of independence for security control Assessors (SCA)?

- A. Business owner
- B. Authorizing Official (AO)
- C. Chief Information Security Officer (CISC)
- D. System owner

**Answer:** B

#### NEW QUESTION 694

- (Exam Topic 14)

Which of the following job functions MUST be separated to maintain data and application integrity?

- A. Applications development and systems analysis
- B. Production control and data control functions
- C. Scheduling and computer operations
- D. Systems development and systems maintenance

**Answer:** D

#### NEW QUESTION 699

- (Exam Topic 14)

Which layer handle packet fragmentation and reassembly in the Open system interconnection (OSI) Reference model?

- A. Session
- B. Transport
- C. Data Link
- D. Network

**Answer:** B

#### NEW QUESTION 702

- (Exam Topic 14)

A financial company has decided to move its main business application to the Cloud. The legal department objects, arguing that the move of the platform should comply with several regulatory obligations such as the General Data Protection (GDPR) and ensure data confidentiality. The Chief Information Security Officer (CISO) says that the cloud provider has met all regulations requirements and even provides its own encryption solution with internally-managed encryption keys to address data confidentiality. Did the CISO address all the legal requirements in this situation?

- A. No, because the encryption solution is internal to the cloud provider.
- B. Yes, because the cloud provider meets all regulations requirements.
- C. Yes, because the cloud provider is GDPR compliant.
- D. No, because the cloud provider is not certified to host government data.

**Answer:** B

#### NEW QUESTION 706

- (Exam Topic 14)

When a flaw in Industrial control (ICS) software is discovered, what is the GREATEST impediment to deploying a patch?

- A. Many IG systems have software that is no longer being maintained by the venders.
- B. Compensating controls may impact IG performance.
- C. Testing a patch in an IG may require more resources than the organization can commit.
- D. vendors are required to validate the operability patches.

**Answer:** D

**NEW QUESTION 710**

- (Exam Topic 14)

What is the PRIMARY benefit of analyzing the partition layout of a hard disk volume when performing forensic analysis?

- A. Sectors which are not assigned to a perform may contain data that was purposely hidden.
- B. Volume address information for he hard disk may have been modified.
- C. partition tables which are not completely utilized may contain data that was purposely hidden
- D. Physical address information for the hard disk may have been modified.

**Answer:** A

**NEW QUESTION 712**

- (Exam Topic 14)

Which of the following would an internal technical security audit BEST validate?

- A. Whether managerial controls are in place
- B. Support for security programs by executive management
- C. Appropriate third-party system hardening
- D. Implementation of changes to a system

**Answer:** D

**NEW QUESTION 713**

- (Exam Topic 14)

Which of the following is the MOST important activity an organization performs to ensure that securiy is part of the overall organization culture?

- A. Ensue security policies are issued to all employees
- B. Perform formal reviews of security Incidents.
- C. Manage a program of security audits.
- D. Work with senior management to meet business goals.

**Answer:** C

**NEW QUESTION 714**

- (Exam Topic 14)

Which layer of the Open systems Interconnection (OSI) model is being targeted in the event of a Synchronization (SYN) flood attack?

- A. Session
- B. Transport
- C. Network
- D. Presentation

**Answer:** B

**NEW QUESTION 719**

- (Exam Topic 14)

How can a security engineer maintain network separation from a secure environment while allowing remote users to work in the secure environment?

- A. Use a Virtual Local Area Network (VLAN) to segment the network
- B. Implement a bastion host
- C. Install anti-virus on all enceinte
- D. Enforce port security on access switches

**Answer:** A

**NEW QUESTION 722**

- (Exam Topic 14)

A new Chief Information Officer (CIO) created a group to write a data retention policy based on applicable laws. Which of the following is the PRIMARY motivation for the policy?

- A. To back up data that is used on a daily basis
- B. To dispose of data in order to limit liability
- C. To reduce costs by reducing the amount of Retained data
- D. To classify data according to what it contains

**Answer:** B

**NEW QUESTION 725**

- (Exam Topic 14)

Which of the following security testing strategies is BEST suited for companies with low to moderate security maturity?

- A. Load Testing
- B. White-box testing

- C. Black -box testing
- D. Performance testing

**Answer:** B

#### NEW QUESTION 728

- (Exam Topic 14)

According to the Capability Maturity Model Integration (CMMI), which of the following levels is identified by a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines?

- A. Level 0: Incomplete
- B. Level 1: Performed
- C. Level 2: Managed
- D. Level 3: Defined

**Answer:** D

#### NEW QUESTION 731

- (Exam Topic 14)

Which of the following is an accurate statement when an assessment results in the discovery of vulnerabilities in a critical network component?

- A. The fact that every other host is sufficiently hardened does not change the fact that the network is placed at risk of attack.
- B. There is little likelihood that the entire network is being placed at a significant risk of attack.
- C. A second assessment should immediately be performed after all vulnerabilities are corrected.
- D. There is a low possibility that any adjacently connected components have been compromised by an attacker

**Answer:** C

#### NEW QUESTION 736

- (Exam Topic 14)

Utilizing a public wireless Local Area network (WLAN) to connect to a private network should be done only in which of the following situations?

- A. Extensible Authentication Protocol (EAP) is utilized to authenticate the user.
- B. The client machine has a personal firewall and utilizes a Virtual Private Network (VPN) to connect to the network.
- C. The client machine has antivirus software and has been scanned to determine if unauthorized ports are open.
- D. The wireless Access Point (AP) is placed in the internal private network.

**Answer:** A

#### NEW QUESTION 739

- (Exam Topic 14)

What are the roles within a scrum methodology?

- A. System owner, scrum master, and development team
- B. Product owner, scrum master, and scrum team
- C. Scrum master, requirements manager, and development team
- D. Scrum master, quality assurance team, and scrum team

**Answer:** B

#### NEW QUESTION 741

- (Exam Topic 14)

Which of the following is the BEST identity-as-a-service (IDaaS) solution for validating users?

- A. Lightweight Directory Access Protocol (LDAP)
- B. Security Assertion Markup Language (SAM.)
- C. Single Sign-on (SSO)
- D. Open Authentication (OAuth)

**Answer:** A

#### NEW QUESTION 743

- (Exam Topic 14)

Which of the following is MOST critical in a contract for data disposal on a hard drive with a third party?

- A. Authorized destruction times
- B. Allowed unallocated disk space
- C. Amount of overwrites required
- D. Frequency of recovered media

**Answer:** C

#### NEW QUESTION 748

- (Exam Topic 14)



Which of the following management processes allots **ONLY** those services required for users to accomplish their tasks, change default user passwords, and set servers to retrieve antivirus updates?

- A. Compliance
- B. Configuration
- C. Identity
- D. Patch

**Answer:** B

#### NEW QUESTION 750

- (Exam Topic 14)

Which of the following practices provides the development of security and identification of threats in designing software?

- A. Stakeholder review
- B. Requirements review
- C. Penetration testing
- D. Threat modeling

**Answer:** D

#### NEW QUESTION 751

- (Exam Topic 14)

Digital certificates used transport Layer security (TLS) support which of the following?

- A. Server identify and data confidentiality
- B. Information input validation
- C. Multi-Factor Authentication (MFA)
- D. Non-reputation controls and data encryption

**Answer:** A

#### NEW QUESTION 752

- (Exam Topic 14)

Which of the following threats exists with an implementation of digital signatures?

- A. Spoofing
- B. Substitution
- C. Content tampering
- D. Eavesdropping

**Answer:** A

#### NEW QUESTION 757

- (Exam Topic 14)

When a system changes significantly, who is **PRIMARILY** responsible for assessing the security impact?

- A. Chief Information Security Officer (CISO)
- B. Information System Owner
- C. Information System Security Officer (ISSO)
- D. Authorizing Official

**Answer:** B

#### NEW QUESTION 760

- (Exam Topic 14)

A security engineer is designing a Customer Relationship Management (CRM) application for a third-party vendor. In which phase of the System Development Life Cycle (SDLC) will it be **MOST** beneficial to conduct a data sensitivity assessment?

- A. Development / Acquisition
- B. Initiation
- C. Enumeration
- D. Operation / Maintenance

**Answer:** B

#### NEW QUESTION 761

- (Exam Topic 14)

Which of the following is a peer entity authentication method for Point-to-Point Protocol (PPP)?

- A. Challenge Handshake Authentication Protocol (CHAP)
- B. Message Authentication Code (MAC)
- C. Transport Layer Security (TLS) handshake protocol
- D. Challenge-response authentication mechanism

**Answer:** A

#### NEW QUESTION 762

- (Exam Topic 14)

An analysis finds unusual activity coming from a computer that was thrown away several months prior, which of the following steps ensure the proper removal of the system?

- A. Deactivation
- B. Decommission
- C. Deploy
- D. Procure

**Answer: B**

#### NEW QUESTION 763

- (Exam Topic 14)

What is the MAIN reason to ensure the appropriate retention periods are enforced for data stored on electronic media?

- A. To reduce the carbon footprint by eliminating paper
- B. To create an inventory of data assets stored on disk for backup and recovery
- C. To declassify information that has been improperly classified
- D. To reduce the risk of loss, unauthorized access, use, modification, and disclosure

**Answer: D**

#### NEW QUESTION 765

- (Exam Topic 14)

Which is the MOST effective countermeasure to prevent electromagnetic emanations on unshielded data cable?

- A. Move cable away from exterior facing windows
- B. Encase exposed cable runs in metal conduit
- C. Enable Power over Ethernet (PoE) to increase voltage
- D. Bundle exposed cables together to disguise their signals

**Answer: B**

#### NEW QUESTION 768

- (Exam Topic 14)

When designing an Occupant Emergency plan (OEP) for United States (US) Federal government facilities, what factor must be considered?

- A. Location of emergency exits in building
- B. Average age of the agency employees
- C. Geographical location and structural design of building
- D. Federal agency for which plan is being drafted

**Answer: A**

#### NEW QUESTION 769

- (Exam Topic 14)

During a recent assessment an organization has discovered that the wireless signal can be detected outside the campus area. What logical control should be implemented in order to BEST protect confidentiality of information traveling over wireless transmission media?

- A. Configure a firewall to logically separate the data at the boundary.
- B. Configure the Access Points (AP) to use Wi-Fi Protected Access 2 (WPA2) encryption.
- C. Disable the Service Set Identifier (SSID) broadcast on the Access Points (AP).
- D. Perform regular technical assessments on the Wireless Local Area Network (WLAN).

**Answer: B**

#### NEW QUESTION 770

- (Exam Topic 14)

Which of the following provides the GREATEST level of data security for a Virtual Private Network (VPN) connection?

- A. Internet Protocol Payload Compression (IPComp)
- B. Internet Protocol Security (IPSec)
- C. Extensible Authentication Protocol (EAP)
- D. Remote Authentication Dial-In User Service (RADIUS)

**Answer: B**

#### NEW QUESTION 774

- (Exam Topic 14)

Change management policies and procedures belong to which of the following types of controls?

- A. Directive
- B. Detective
- C. Corrective
- D. Preventative

Answer: A

Explanation:

Reference: <https://books.google.com.pk/books?id=9gCn86CmsNQC&pg=PA570&lpg=PA570&dq=CISSP+Change+mana>

NEW QUESTION 776

- (Exam Topic 14)

Match the level of evaluation to the correct common criteria (CC) assurance level.

Drag each level of evaluation on the left to its corresponding CC assurance level on the right

Level of Evaluation

Structurally tested

Methodically tested and checked

Methodically designed, tested, and reviewed

Functionally tested

Semiformally verified design and tested

Formally verified design and tested

Semiformally designed and tested

Assurance Level

1

2

3

4

5

6

7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Level of Evaluation

Structurally tested

Methodically tested and checked

Methodically designed, tested, and reviewed

Functionally tested

Semiformally verified design and tested

Formally verified design and tested

Semiformally designed and tested

Assurance Level

1

2

3

4

5

6

7

Functionally tested

Structurally tested

Methodically tested and checked

Methodically designed, tested, and reviewed

Semiformally designed and tested

Semiformally verified design and tested

Formally verified design and tested

NEW QUESTION 778

.....

## Relate Links

**100% Pass Your CISSP Exam with Exam Bible Prep Materials**

<https://www.exambible.com/CISSP-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>